AU/ACSC/MILLER/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

UNDERSTANDING THE UNIQUE CHALLENGES OF THE CYBER DOMAIN

by

Kenneth J. Miller, Major, USAF

A Short Research Paper Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Instructor: Lieutenant Colonel Mark Black

Maxwell Air Force Base, Alabama

March 2010

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

Abstract

The mission of the United States Air Force is to fly, fight and win…in air, space and cyberspace. On December 7, 2005 the Air Force Chief of Staff added the word "cyberspace" to the Air Force mission statement and ever since Airmen have struggled to clearly define and better understand the cyberspace domain. In his book, Strategic Warfare in Cyberspace, Lt Col Gregory Rattray took a historical perspective and offered an interesting comparison between the development and advancement of air power in World War II and today's emergence of strategic warfare in cyberspace. While Lt Col Rattray's approach yielded many similarities between the development of air power and the development of cyber power, it is important to highlight that the air and cyber domains are two very different operating environments. The primary aim of this paper is to highlight some of the unique challenges the cyber domain presents. By better understanding these unique challenges we can better prepare to fly, fight and win in cyberspace.

INTRODUCTION

The United States Air Force must be prepared to confront new challenges while conducting operations in the cyber domain. These new challenges arise from the fact that the cyber domain is very different from the other warfighting domains. The primary challenges we must understand include the lack of situational awareness in the cyber domain, the ineffectiveness of deterrence in the cyber domain, the classification of the network as a weapon system, the balance between network security and operational convenience, and the dangers of social media. Given these five unique challenges, our Air Force leadership must begin to develop and grow our future force to possess a sort of cyber-mindedness in order to fully understand and exploit the capabilities of this new operating domain. Similar to the concept of "air-mindedness" already imbued into every Airman, cyber-mindedness involves the unhindered development of cyberspace capabilities to achieve desired effects.[1]

THE LACK OF CYBER SITUATIONAL AWARENESS

The cyber domain warrants a much stronger defensive posture than any of the other warfighting domains due to the lack of cyber situational awareness. Before we discuss the many reasons for the lack of cyber situational awareness let's provide a common, working definition of situational awareness. Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.[2]

The physical and geographic boundaries that clearly delineate the limits of the land, sea, and air domains do not exist within the cyber domain. This lack of boundaries within the cyber domain prohibits us from being able to clearly define the cyber domain, contain the cyber

domain, and produce a common operating picture of the cyber domain. Additionally, the ability for anyone to enter and exit the cyber domain anonymously further complicates any attempt to control the domain, let alone achieve any degree of cyber superiority. Within our air domain we have identification, friend or foe and within the land domain we have Blue Force Tracker to enable our forces to keep track of who is who and provide situational awareness. However, within the cyber domain it is not as easy to provide for situational awareness. While we can attach certificates to our e-mail to allow others to know they are legitimate, we have no way of identifying the millions of other users who we share the cyber domain with at any given moment. Additionally, due to the ever changing nature of the domain, it is virtually impossible to create a common operating picture. This inherent inability to establish cyber situational awareness will continue to require us to maintain a strong defensive posture in cyberspace.

CYBER DETERRENCE IS INEFFECTIVE

It is important to understand why traditional deterrence is not an effective defensive strategy in the cyber domain. A significant issue for deterrence is that because such cyber attacks can be launched in secret, the identities of the actors carrying them out often cannot readily be determined. For example, a cyber attack seemingly originating in China might have been launched by the Chinese government, by some unofficial group of hackers in China or elsewhere, or by terrorists in the Middle East who disguise their identities. The alleged but ambiguous Russian cyber attack on Estonia is another obvious example.[3] The main reason that deterrence is ineffective is our inability to directly attribute specific actions to a specific actor within the cyber domain.

Regardless of the strength of our nation's offensive capabilities, if we cannot directly attribute an attack to a specific actor, we cannot retaliate against it. Throughout history the weapons used in warfare have evolved and grown more and more deadly. However, there always remained a way to link an effect to an action and an action to an actor. In today's cyber domain this is not always possible. Take for example, a malicious information packet transiting the cyber domain. Unlike weapons of the past, today's cyber packet lacks any forensic characteristics such as fingerprints, ballistics, or DNA. While some sophisticated technology can attempt to trace the packet back to its point of origin the speed and range of operations in cyber space and the ability to mask and cover up one's tracks prevents us from truly being able to attribute an action to a specific individual. The cyber domain within which we operate today is comparable to the American wild west of the 1800s. Given the lack of attribution and the boundless range of the cyber domain, we cannot depend upon deterrence to protect us from our enemies in cyber space.

THE NETWORK AS A WEAPON SYSTEM

The Air Force must strengthen its emphasis on treating the network as a weapon system. We place so much emphasis on the protection of our classified networks, when in fact it is our unclassified networks that we depend upon for the majority of our day to day operations. A skillful enemy could likely wreck just as much havoc targeting an unclassified system as he could if he targeted a classified system. Our enemy's ability to achieve similar effects regardless of the classification level of the network underscores our need to equally protect all network systems regardless of their classification level. It makes no sense to have different standards and protocols for different systems just because they handle different classifications of material. We

should apply our toughest standards across all of our classified and unclassified network systems and not allow classification to determine a system's level of protection. The only difference between systems should be who has access to them and that network access should depend upon an individual's security clearance and their need to know. We cannot afford to maintain different standards for different networks solely based upon the classification of the material on the network.

BALANCING SECURITY AND CONVENIENCE

The Air Force must continually strive to maintain an acceptable balance between network security and operational convenience. The demonstrated capabilities of our enemies in the cyber domain warrant a strong defensive posture. However, our growing demand and reliance upon the cyber domain for our day to day operations requires an increasing amount of flexibility and openness. Given our desire for operational convenience, one of our greatest security vulnerabilities arises from our ability to connect to the .mil domain from home.

Advocates of the ability to connect to the .mil domain from home argue that potential security vulnerabilities are mitigated through the use of the Common Access Card. The Common Access Card utilizes individual certificates and encryption to provide authentication for those users who connect to the .mil domain from their home computers. However, even if a remote connection is authentic and the data encrypted, the connection represents a backdoor into our .mil domain that is vulnerable to exploitation.

Unfortunately many of our Airmen do not provide the same level of protection for their home computers as the Air Force does for their government computer. Therefore if a virus existed on an individual's home computer it could pass easily from the individual's home

computer to the .mil network via the remote connection. Unfortunately, the growing desire for the ability to connect to the .mil domain while traveling and from home will continue to challenge our security experts. The balance between providing network security and operational convenience will also challenge our senior leadership as they develop policies that protect our Air Force networks while allowing for the increased flexibility our workforce demands. The underlying rational for nearly all requests for remote access to the .mil domain is the requesting individual's desire for convenience. There does exist a few valid requirements for remote access for senior leadership and other specific operational needs, however, for the majority of the workforce the convenience of being able to work from home has grown to outweigh the Air Force's concern for securing the network.

THE DANGERS OF SOCIAL MEDIA

The Air Force recently decided to allow access to social media from the .mil domain. In doing so, the Air Force must also develop ways to carefully monitor the explosive use of social media within the .mil domain to highlight and address potential vulnerabilities. Previously, most military networks prevented access to social media pages, personal e-mail, and other types of non-mission essential traffic. The demand for social media connectivity will likely grow and cause increased competition between those who wish to keep the network locked down and those who need access to social media sites necessary for their specific mission. In addition to the demand for network access to social media, there also exists vulnerabilities in what our military personnel share via these media channels.

The type of personal information shared on websites such as Facebook include detailed information about one's family, vehicles, home, finances, calendars, photo albums, and

numerous other subjects. Given an adversaries' desire to gather information about a particular person of interest, they need to look no further than the person's Facebook page. Recently, Canadian and Australian officials urged soldiers and civilian workers to be mindful about what they post for the world to see. Canadian Army Brig. Gen. Peter Atkinson said in a United Press International article that insurgents collect about 80 percent of their intelligence from blogs and photos posted on social networking sites like Facebook and YouTube.[4] Armed with this personal information, a potential enemy could use it for blackmail, to disrupt financial transactions, alter morale, target movements, predict behavior, and even map other social networks. For a perfect example of this type of cyber exploitation we need to look no further than the Persian Gulf War when the United States targeted the e-mail accounts and cell phones of Iraqi leadership in an attempt to launch an information war prior to launching the conventional war. While the benefits of various social media are well documented and proven in the commercial business world, I am still concerned that social media offers yet another avenue for enemy exploitation.

CONCLUSION

In conclusion, the United States Air Force must better prepare to confront a new set of challenges while conducting operations in the cyber domain. The primary challenges we must understand include the lack of situational awareness in the cyber domain, the ineffectiveness of deterrence in the cyber domain, the classification of the network as a weapon system, the balance between network security and operational convenience, and the dangers of social media. These new challenges that I highlighted arise from the fact that the cyber domain is very different from the other warfighting domains in which we have become acclimated. The combination of these

challenges will require our Air Force leaders to take action and work to better understand this new operational domain.

[1] Lord, USAF Cyberspace Command, 14
[2] Salerno, A Situational Awareness Model Applied to Multiple Domains, 17
[3] Kugler, Deterrence of Cyber Attacks, 317
[4] Wright, Officials Urge Caution on Social Networking Web Sites, 2

Bibliography

Kugler, Richard L. "Deterrence of Cyber Attacks." Cyberpower and National Security.

Lord, William T. "USAF Cyberspace Command." Strategic Studies Quarterly. Fall 2008.

Salerno, Hinman, and Boulware. "A Situation Awareness Model Applied to Multiple Domains." In Proceedings of the Defense and Security Conference, Orlando, FL. March 2005.

Wright, Ashley M. "Officials Urge Caution on Social Networking Web Sites." Air Force Print News. April 2008.